conclusions and recommendations section, I summarize the relevant ones here to set the record straight immediately on this matter. I recommend:

e.1 Retain the existing industry authentication standard exactly as it now is. Do not make any changes in the implementations of authentication in cellular switches or IS-41 networks. If it is not already clear to the reader, this is completely compatible with the general thrust of my other comments and suggestions and totally contrary to what AWS's accuses.

e.2 Rewrite Rule 22.919 to require manufacturers to incorporate authentication in all new set production, both newly type-accepted designs and, as soon as feasible, continuing production of non-authenticating types which were previously type accepted.

e.3 Furthermore, encourage the production of the most secure form of authentication, namely the separable chip. This would imply that the rule consistently allow specific instances of moving or copying the same ESN into more than one set, when owned by the same valid cellular customer.

e.4 For older sets which can only be practically upgraded via software changes, again permit a specific instance of moving or copying the ESN parallel to the previous case, but again restrict this to only sets owned by the same valid cellular customer. In connection with this last instance, require upgrading the software/firmware in the set as well, for each set having suitable software/firmware upgrade available. All of this is again completely consistent with the present industry authentication standard, without modification.

8. AWS asserts (page 10 and 14-15) that the existence of two extension cellular phone sets with the same MIN/ESN would interfere with the ability of carriers to intercept, to the exclusion of any other communications, the electronic communications of a [targeted] customer as mandated by CALEA. AWS asserts that this would even occur even if a targeted customer used only one of several extension sets at a time. This claim is made without substantiating background information or data. In the absence of any technological reasons to support this assertion, and based on my knowledge of the technology of cellular and PCS systems, I must conclude that this AWS assertion is technologically incorrect.

Again, any possible reasons for AWS's response are beyond my understanding. When a carrier is served with a valid court order to intercept and make available to a designated law enforcement agency the communications of a targeted individual or organization, there is no technological or operational reason why the existence and use of any number of extensions or MUSDN phones by that individual or organization should, in any conceivable manner, impede or affect the ability to completely and promptly respond and provide the requested interception(s). This is also true even in the case (not mentioned by AWS) when the targeted individual improperly uses multiple cellular telephones with the same MIN/ESN simultaneously and even if the base system permitted connection of both conversations.

In all cases, should only persons not covered by the court order be engaged in the targeted intercepted conversation, the operational treatment of this situation will be exactly like the corresponding case in a landline interception. The non-targeted conversations will be excised from the material legally used, and otherwise treated accordingly.

9. AWS asserts 9 specific allegedly costly obligations which would be placed on the carriers as a result of permitting use of cellular extension phones (page 15-16). Without repeating the wording of each of the 9 assertions, I will respond to them in the same numbered order. The reader may need to refer to the AWS document for the corresponding assertion.

9.1 AWS alleges that cellular extension telephones will have improper multiple registration or paging response messages (due to improper simultaneous power-up use) to such an extent that additional carrier staff and resources will be required to handle the resulting situation. Again, the corresponding case of MUSDN simultaneous use is not mentioned. Although the technological details of the two cases are not completely identical, one would assume that the probability of improper simultaneous power-up and consequent duplicate registration or paging response of two MUSDN sets should be approximately the same as for extensions. Therefore, AWS should be put to its proof based on existing MUSDN data to substantiate that the number of such events is sufficient to support this assertion. If no quantitative proof is forthcoming, it is not possible to quantify this assertion, and I can only conclude that the level of such undesirable signaling channel messages is no greater than the level created by MUSDN sets, which AWS and other carriers must find acceptable since they support MUSDN service. See further comments on MUSDN below.

9.2 AWS alleges necessary extensive and costly revamping, due solely to emulated extensions, of the still-unfinished RF fingerprinting or RF signature anti-fraud systems now under evaluation. First, my evaluation of the complexity and cost of the modifications required due to the actual changes required

by multiple extensions is clearly vastly smaller quantitatively than those implied by AWS, although no dollar figures have been stated by either side in these filings to date. In my view, the first step in considering such an assertion of high costs associated with an experimental system must be a binding statement by AWS and/or other relevant carriers, once they have completed evaluation and testing, committing them to purchase stated dollar amounts of RF signature equipment for their entire network, not just a few cells here and there. Until this happens, we must view this as a remotely possible but not very probable situation, not worthy of consideration as a meaningful obstacle to the changes in Rule 22.919 which I favor. Once full network implementation of RF signature equipment is a done deal, then it is possible to proceed to examine quantitatively the added resources required by the existence of multiple cellular extension phones, substantiating any claims with hard evidence.

My present view is that the only definite added human interface operational cost for the portion of activation related to RF Signature/Fingerprint equipment is to type the digit "2" (or 3 or 4, or whatever) in the data entry field when a customer signs up for service, and the de minimus cost of an additional waveform data entry internal to the RF Signature/Fingerprint equipment's memory, for each additional operative cellular phone. Surely this does not require hiring extra staff, as AWS asserts. I have the present view that the total additional cost of supporting multiple extensions on RF signature equipment will also be de minimus. However, since it is clearly a minimal additional cost for one set or for MUSDN sets, I see no reason why the multiple extension customer should not pay this minimal extra cost for data memory for each additional set, as was already suggested by Tim Fitzgibbon in a previous letter to the Commission. In short, although I am open to further information which may modify my view, I do not find any basis to justify this as an additional extraordinary or even significant cost for the carrier.

9.3 AWS asserts that industry standard authentication must be abandoned if carriers are to offer service to emulated extensions, a doubly wrong statement covered in detail in my section 7.3.e above. Since it is based on a total misconception by AWS as noted above, it is, in my view, not applicable.

9.4 AWS asserts incorrectly that an existing call (of another extension phone owned by the same customer or of an unrelated conversation) will be dropped or degraded in quality if the extension owner improperly attempts to start another call while the first call is in progress. These incorrect technological assertions were discussed and rebutted in detail in my 1995 report, which AWS affirmed in the July 1995 meeting. Under no circumstances will a properly functioning cellular system drop an existing call of any type because a new call of any type is initiated. Under no circumstances (with the possible exception of emergency overload operational mode*) will a properly functioning and competently operated cellular system block or degrade the service of other customers because of the attempt to setup a call by another phone. Because this assertion is completely false and is based on a false assumption, it is not applicable.

9.5 AWS asserts that some as-yet-undefined new cellular service development is required as a prerequisite to giving continuing service to extension cellular sets. This is false. The present treatment of two sets with the same MIN is well defined and it is this: if one such cellular phone is already engaged in a call, the others cannot begin a call. This applies equally to both extension sets and MUSDN sets. Therefore from the point of view of using this to justify an alleged costly development, it is not applicable.

However, in consideration of the possibility that this statement by AWS may represent a breakthrough compromise action between the opposing sides on this issue, there is also the possibility that it would be desirable for the industry to define some new feature in call processing for extensions. This would, of course, apply to both emulated extensions and to MUSDN equally, since both are presently unable to have two sets participate in the same call at present. For example, perhaps it is desirable that two extensions may be used simultaneously and automatically conferenced in the same call so that their operation would then be more similar to landline extensions. While this is not obviously the desired approach, this matter should be referred to a standards committee for further study.

---

* In emergency overload mode, certain cellular phones such as a government official(police, military, etc.), designated health care providers (certain ambulances, certain specifically certified emergency care physicians, etc.) or cellular carrier executive's or repair staff's cellular telephone are treated with higher priority than ordinary users. Ordinary users are blocked or restricted in making new calls. The quality of all ongoing calls is not affected. This has absolutely no connection whatever with emulated extension or MUSDN cellular phones.

It is encouraging that a carrier such as AWS is apparently willing to examine the possibility of other types of call handling for extensions and MUSDN sets, and I agree with AWS that other types of call processing which are more useful to the customer are of interest and are worth investigating.

9.6 In responding to this point, I admit that I am not completely sure that I understand the assertion of AWS, and I am prepared to stand corrected if this is so. I take this point to be an objection that there is a resource burden on AWS and similar carriers to respond "immediately" if they have objections to activation of emulated extensions for a particular customer. If this is a correct interpretation of this assertion, then I feel that it is not appropriate. I have checked with several sales agencies which market AWS service here in my own Dallas area, and they all confirm that AWS will respond to them within the half-hour for well over 90% of all applications for service, if AWS has any objection to that customer such as bad credit rating, questionable identification or other reasons. Given that AWS is already responding in a time that would fit the word "immediately" quite accurately for most customers today in the normal course of business, it is unreasonable to allege that doing so in the future represents an extraordinary drain on their resources above and beyond what they are doing as a matter of course today.

9.7 AWS asserts special problems to comply with CALEA for emulated extension cellular phones. This assertion is apparently based on a misconception by AWS as described in my section 8 above, and is in my view not applicable.

9.8 AWS asserts extraordinary and/or unpredictable traffic burdens due to emulated extensions. This assertion is apparently based on a misconception by AWS which was rebutted in great detail in my 1995 report, and is in my view not applicable. Again, AWS specifically assented to the 1995 report in the July 1995 meeting.

9.9 AWS asserts an extraordinary burden to write customer contracts for emulated extension customers. This assertion is clearly a de minimus cost item. AWS and other carriers have competent full time legal staff members who can, and do in fact, frequently draft a variety of new special customer contract forms without alleging that this produces an extraordinary or excessive internal expenses. Therefore, in the absence of any reason why this contract should be so much more costly to draft than all others, I feel that it is not an applicable objection.

Again, in connection with these 9 points, I feel that it is important to note that AWS incorrectly alleges a number of developments which it claims are required to support emulated extensions, while it does not indicate that the same developments would be required for support of MUSDN. In addition, they completely omit one very important case which cuts the opposite way. Emulated extensions presently work correctly in conjunction with the IS-41 cellular network and thus they can receive proper roaming service throughout the North American cellular network. In contrast, MUSDN secondary cellular phones are incompatible with the IS-41 North American cellular network, since its fundamental architecture is based on a one-to-one relationship between a cellular phone's MIN-ESN pair value, whereas MUSDN sets violate this by having the same MIN in two sets but with different ESN values in the two sets. The high cost of the "wholesale revamping" of the cellular network to support MUSDN cellular phones is nowhere mentioned by AWS, although there would be no corresponding economic cost for emulated extensions since they roam correctly in the North American cellular network already without any new development required.

To recap, of the 9 specific extraordinary operating expenses asserted in this section, I view six of the nine assertions as not applicable due to either a false underlying assumption on the part of AWS, or on an assumed service development effort which does not, in fact, exist. In one case I assume that the cost of providing the response time to activation objections consistent with AWS's present response time is not an extraordinary burden justifying added costs, but I am not confident that I understand the corresponding statement in the AWS letter fully. In addition, most of these items are assertions which were rebutted fully in my 1995 report, which was accepted without objection by AWS in July 1995. One of the remaining assertions is based on assumption which is testable comparison to MUSDN which is discussed further below, and I put AWS to their proof on this matter. One of the assertions is speculative since it involves an experimental system which may or may not finally be widely used in the cellular network, and if it actually used I seriously question the implication of high cost and system disruption made by AWS and ask for their proof. Finally, I view the last item as a de minimus normal cost of doing business. I believe that these items do not justify a claim of huge cost burdens to the carrier.

10. AWS asserts a number of alleged defects in the proposed rules and procedures put forth by C2+ (page 17-18), presumably referring to the same cover letter by Tim Fitzgibbon which I have referenced. Although these are operational rather than purely technological, I feel that it is appropriate to respond to them for completeness and consistency of my message.

10.1 AWS asserts that anyone can clone a phone lawfully under the rules proposed by C2+. My understanding of the specific procedural and operational methods proposed by Mr. Fitzgibbon to be used by vendors offering extension service, would prevent unrestricted use of the equipment by mandatory use of encrypted transfer,

central data bases, and other well-proven methods which appear to be technologically superior to the purely "locked door" and "erase before write" protective methods used by the authorized repair depots of the manufacturers. I agree that totally unaccountable changing of ESNs by anyone, anywhere, is not in the public interest and that adequate controls should be in place to prevent this, but I believe that the rules and methods proposed by Mr. Fitzgibbon are adequate for this purpose.

10.2 AWS asserts that the emulator would not be held accountable for mis-instructing the customer or other errors. Again, my understanding of the procedures proposed by Mr. Fitzgibbon did not unfairly protect the emulator from just responsibility and accountability for any errors, omissions or wrongdoing, and I agree that all parties involved in the process should be held properly legally responsible for their proper actions.

10.3 AWS asserts that the procedure proposed for notifying the carrier of emulation is a "license for subscription fraud." Again, my view is that the emulator is following the same steps as the carrier or the other sales agents of the carrier to verify that the customer is properly identified and is a valid customer of the carrier. Furthermore, under the procedures proposed by Fitzgibbon, the emulator gives the carrier written notice so the carrier can respond if there is any perceived problem regarding this particular customer, who is, significantly, already known to the carrier. I cannot find why this is a "license for subscription fraud," when the existing procedures of the carrier's own present sales agents are the very same.

10.4 AWS complains that the proposed procedures place the entire burden of the carrier to police the system for simultaneous registrations, but objects that there is a dispute about the number of such simultaneous registrations which is likely to occur. First, in direct response to the stated question, AWS is quite naturally assuming that only the carrier will monitor the use of the radio channels, because this is an ongoing result of operating the cellular switch, which stores all manner of historical message and traffic data in the normal course of business. I must agree that everyone is looking to the carrier for this type of information because the carrier produces it normally. In fact, if my suggestion (in section 13.a comments below) to restrict monitoring of the cellular setup channel were codified into law, a third party would need to justify any monitoring of the setup channel, even if the purpose were only to gather independently the information already gathered by the carrier. At another level, this leads to some additional significant questions which I will take up in the conclusions.

As this particular allegation is once more based on the stated assumption by AWS that improper simultaneous extension use will be frequent and uncontrollable with emulated extensions, but no mention is made of the comparable incidence expected with MUSDN, I will take this point up again in my comments on MUSDN in the conclusions.

11. **BellSouth Cellemetry ® and its Relevance to Rule 22.919:** Appendix A is a brief summary of a technology developed and owned by BellSouth Wireless, Inc. As the summary explains, this technology uses existing cellular networks to transmit remote measurements (traditionally called "telemetry") via the cellular network, to a "home" data base connected to a "home" MSC. A typical application of Cellemetry ® is to send a signal each time an item (such as a can or bottle of soft drink) is dispensed by a vending machine in a remote location, so that the owner of the vending machine will know when to restock it with product. Transmissions from the Cellemetry ® CRAD cellular phone can also be initiated periodically by a clock mechanism instead of as the result of an unpredictable event. To my current knowledge, this technology is already in use in the service areas of many different cellular operators. Operators charge the end users a fee for use of Cellemetry ®, in addition (in some cases) to providing the Cellemetry ® CRAD cellular radio equipment used at the remote locations.

11.1 First, I must say outright that the technology involved in Cellemetry ® is novel. audacious, and intriguing, and is an admirable invention for effectively utilizing the existing cellular network to provide a data communication link. My purpose in bringing Cellemetry ® into this discussion is not to hinder its further appropriate use and development. In fact, I will propose particular exceptions within Rule 22.919 in my conclusions to ensure that Cellemetry ® can continue to operate legally. At the same time, based on my technological analysis of the Cellemetry ® sytem, I disagree with several of the claims made in Appendix A, and I have great concern that the development of Cellemetry ® has several significant implications regarding the present dispute about Rule 22.919.

11.2 Based on my past detailed analysis of cellular setup channel capacity constraints, and my understanding of the Cellular system, I disagree with the second sentence of page 1 and the top paragraph on page 3 in Appendix A, which claims that "at no time does the Cellemetry ® system impose any significant capacity restraints on the cellular telephone system." Without repeating all the reasons in detail, the algorithm for control of Cellemetry ® transmission requires that the setup channel be "quiet" for a specified time before the Cellemetry ® CRAD cellular radio will transmit. However, no device can predict the future, and there is no way to prevent ordinary cellular radios from also trying to transmit at the same time as the CRAD, regardless of the presence of a prior quiet interval. In a typical situation in which there are highs and lows of setup channel traffic, there will be peaks of ® CRAD cellular radio setup channel transmissions after each interval

of "quiet" on the setup channel. This can cause repeated "collisions" with ordinary cellular phone call processing messages, leading to delays before the cellular phone can try again, and in the most serious case, to aborting the initiation of regular cellular phone calls in that cell as a result. Furthermore, the CRAD transmissions are controlled by an internal clock or by an unpredictable event, rather than by the normal timing control parameters which are broadcast by the cellular base station. Therefore, to a certain extent, the carrier does not have the type of control over autonomous registration messages from the CRAD which the carrier has over ordinary cellular phones. All this leads to a setup-channel traffic impact, and a number of related questions regarding the assertions by the CTIA and by AWS in the current proceedings, and their prior allegations regarding alleged impact on the performance of cellular systems by such alleged problem situations as multiple registrations or other setup channel signals from emulated extensions. Although I was under the impression that these allegation had been adequately rebutted in my 1995 report, they have surfaced again in the form of the various current allegations by AWS that there will be uncontrollable multiple registration messages from multiple extension cellular phones, and various dire consequences arise from that which lead to complexity and expense in the network, need for staff and other resources, etc.

While I do not want to exaggerate the level of problem which can result, it is significant to note that Cellemetry ® equipment can in fact be truly responsible for the very type of multiple registration and other setup channel activity which AWS incorrectly asserts are deleterious aspects of the use of extension telephones (but which I contend would only happen with improper simultaneous power-up of multiple extensions). There is no coordination between different installed Cellemetry ® CRAD cellular radios, and there is no way to prevent several of them in different locations from sending a registration message simultaneously. Even in the case where the timing of the Cellemetry ® CRAD cellular radio's transmission is controlled by a clock, it could interfere with setup channel signals from ordinary single cellular sets, since there is no coordination between the two. I fully recognize that the potential problem with ® CRAD cellular radios can be minimized by carefully coordinated placement of these devices, but great care must be taken to limit the number and placement of ® CRAD cellular radios in each cell or sector, based on their expected traffic, to try to control this adverse effect on the setup channel. If CRAD placement is done without great care, a problem can indeed result.

One preferred implementation of Cellemetry ® is to use the same "fake" MIN for all the Cellemetry ® CRAD cellular radios associated with a particular cellular operator, regardless of their installation location. As a result, they will all produce IS-41 network messages back to the same home MSC, without using up all the allocated telephone numbers for that MSC or duplicating MIN values assigned to real customers. Therefore, their appearance to the network and base stations is like a flock of un-coordinated cellular radios with the same MIN telephone number, which could often all simultaneously send registration messages on the setup channel. These are the precise things which AWS in particular objected to and claimed would be a major problem with emulated extensions. It is then significant to inquire why the same type of multiple registrations are so objectionable to the carrier when they are produced only by improperly simultaneously power-on emulated extensions (and thus their quantitative occurrence is a matter of dispute, requiring a mistake by the customer), but the same type of signals are strangely acceptable to the carrier when they are produced by <u>normal operation</u> (not a mistake in their use) of equipment for which the carrier receives extra revenue, or for that matter, when they are produced by the same type of mistaken simultaneous power-on of two MUSDN sets.

11.3 One of the most important relationships of Cellemetry ® to the discussion of Rule. 22.919 is that a Cellemetry ® CRAD cellular radio can only perform its intended function by intentionally and repeatedly violating Rule 22.919 each and every time it transmits. Its very existence is a violation of the rule, since the ESN value in memory is constantly changing. Not only that, but it also intentionally violates the predecessor rule 22.933. This is a result of the fact that the ESN in its memory and the value transmitted by the CRAD cellular radio is <u>not</u> a fixed value set at the factory, but is in fact a variable such as the number of soft drink cans remaining in a vending machine. Under certain circumstances, when all 32 bits represent the telemetry data value for example, there is no way to prevent two or more CRAD cellular radios from producing the same MIN/ESN values in their unrelated (and possibly nearly simultaneous) registration signals on the setup channel. Apparently the cellular operators do not object to this.

Clearly, the Cellemetry ® CRAD cellular radio requires a specific exemption in Rule 22.919 in order to operate legally, and I believe that such an exemption should be included in the rule to permit the valid operation of this device and others like it which perform a useful function and which, when properly and competently provisioned in the system, have a small but not overly deleterious effect on the cellular network. If the cellular operator is willing to tolerate the amount of uncontrollable setup channel traffic produced by a reasonable number of installed CRAD units and there is not an unjust amount of system degradation which would affect the ordinary cellular customers of the system, then the operator should be permitted to get the extra income arising from the installation of the CRAD cellular radios. However, for consistency, the operator should not then be allowed to selectively assert objections to other types of equipment which, only in the case of serious improper use, would produce precisely the same types of signals as the Cellemetry ® equipment. Particularly when these devices such as emulated extensions and MUSDN extensions do <u>not</u> produce any extra setup channel messages when used properly.

11.4 Related non-technical Issues. Aside from the purely technological issues related to Rule 22.919 which are involved in the use and operation of Cellemetry ®, there are some non-technical issues relevant to the current dispute which must be considered at this point.

To my knowledge, the very existence and the widespread use of the Cellemetry ® system has not previously been brought before the Commission in connection with Rule 22.919 by any other party to this docket, despite its obvious relevance. I only learned of its existence and its means of operation in June, although I was aware before that that BellSouth and other carriers had a telemetry system operating via the cellular network for more than a year prior to this, and possibly longer. Before that I assumed it used a traffic or voice channel. BellSouth has apparently made extensive presentations seeking to license this technology to other carriers, and has in fact negotiated several such licenses. Therefore all the cellular carriers such as AWS, and likely the CTIA as well, should have been aware of Cellemetry ®. Assuming this is true, it is necessary to raise the question of why neither they nor any other carrier ever came forward to request an exemption from Rule 22.919 or its predecessor rule so that Cellemetry ® could be legally installed and operated.

Some proponents of the Cellemetry ® system have claimed that Cellemetry ® CRAD cellular phones should be automatically exempt from the old Rule 22.933 and the new Rule 22.919, and furthermore they argue that the proponents of this technology have no responsibility to bring this item to the Commission to request an exemption, because a CRAD generally does not have voice channel capabilities and would not respond to a voice channel assignment command signal from a base station, if such a signal were transmitted. I disagree. There is no excuse for this in one special case when another case is being contested. CRAD radio units all have the ability to scan the various radio channels, since each cell uses a different channel for setup purposes. They must meet type acceptance emission masks to prevent harmful interference to other cellular radios. It is well known that the emission mask for FSK setup channel transmissions have more adjacent channel emission than voice channels do, and the injudicious geographical placement of a CRAD unit could cause interference with all mobile unit call setups or paging responses from that cause alone, aside from the possible co-channel simultaneous transmissions described above. To permit the legal operation of Cellemetry ® equipment, there must be both a specific exemption in Rule 22.919 and also a prohibition against manufacture or alteration of a Cellemetry ® CRAD set so that it could use a voice channel or even interfere with a voice or traffic channel in any way. To do otherwise is to open yet another technological loophole for criminals to evade prosecution. In addition, if there is interference with call setup of ordinary cellular phones from this cause, either due to co-channel or adjacent channel interference, the ordinary customer normally has no way to learn that the cause of bad service is because the carrier has permitted too many CRAD units in one cell. This point is related to the question raised in the following paragraph. Given adequate controls on the provisioning, setting of timer controlled transmissions, etc., however, it is likely that a properly sized group of CRAD units in a cell can do its telemetry job effectively with only minimal effect on the setup channel.

11.6 The topic of Cellemetry ® also again raises the related questions regarding who is responsible for observing the proper use of the cellular band, and what motivation each involved party has to bring all the relevant information about its use before the Commission.

12. **Conclusions:** Clearly the Commission has been historically moving from a past "micro-management" policy of the carriers to a future non-directive policy in which licensees will be given a very free hand regarding the technology of radio band use, and competition rather than detailed regulation will be the basis for control of prices and services offered. I support this and view it as a positive method to increase innovation and use the Commission's resources more effectively. However, in several ways (which I have alluded to before) the carrier "holds all the cards," and when forces of competition alone, given the limited number of competitive carriers, do not produce the best service at the lowest fair and compensatory price, the Commission must still investigate and act in such matters and set them right if the facts merit this. In this particular case, my information is that some carriers have tolerated emulated extensions in the past to varying degrees and some have not, but that recently, and particularly when MUSDN was offered by a carrier in a particular market, aggressive action was then taken by both carriers to prevent and remove emulated extensions, and the consumer had no competitor to turn to in that market.

The Commission's view of what is happening in the cellular and PCS industry should not be molded by the vision of only one party; neither the carriers nor by adversaries. But when disputes arise, the carriers are often in a unique position of holding the necessary information. For example, cellular carriers produce all the operational data regarding the cellular system, in the normal course of business, on magnetic disk or tape as an automatic byproduct of operation of each MSC. When a cellular carrier makes a claim such as "excessive simultaneous registration messages will occur with emulated extensions," that carrier is in a unique position of having the data to either substantiate or not substantiate the allegation, and should be obliged to either present the supporting data or just not make the unsubstantiated claim. More on this point below. Similarly, when an adersary needs such data to refute or disagree with the carrier's position, the carrier should be required to produce it under appropriate controls to protect the legitimate interests of the carrier. This also applies to operational information not produced by the MSC, such as the CTIA claim that no problems have materialized regarding repair or replacement of cellular phones since January 1, 1995.

In another type of issue, if a carrier raises the objection that a certain proposed change in the rules would have an adverse effect on a proposed anti-fraud method which is under evaluation by the carrier(s), then it is necessary to have some factual information placed before the Commission regarding the efficacy of the proposed method and the likelihood that it will actually achieve widespread use. Without this information, one is entitled to a certain level of skepticism regarding whether the carrier is sincerely concerned about interaction of the proposed rule change with the proposed anti-fraud method. It may be that there is no serious plan by the carrier to use the proposed anti-fraud method, but it merely serves as a convenient basis for arguing against the adversarial position. For example, in this filing, I have asked that the carriers make a firm commitment to actually install and use a particular anti-fraud method in their entire system as a precondition to continued discussion of that particular method in this controversy. I specified the "whole system" because, in this case, the carrier's objection was that the problem related to the overall networking aspects of this anti-fraud system. Now, in all fairness to the carrier, the evaluations may be at such a preliminary stage that, while the proposed anti-fraud method is now promising, it is not yet reasonable at this stage to make a business commitment to it. In such a case, the carrier should be required to present the relevant performance data available from testing (not merely claims by the vendor of the proposed anti-fraud method). The Commission's own staff can then draw their own conclusions about how seriously to consider the proposed method. For example, if a proposed anti-fraud method allows 20% of the actually fraudulent calls to get through, and incorrectly blocks 10% of all valid calls placed, then I believe that a reasonable conclusion is that it is not acceptable for general use. Conversely, if another anti-fraud method allows only 1% of actually fraudulent calls to go through, and incorrectly blocks only 1% of all valid calls placed, then this margin of error is within the 2% blocking grade of service required by cellular systems, and this level of technological performance qualifies this second example system for general use. Judgments of this type must, of course, also be tempered by the cost of the proposed system, since some systems are very accurate but are also very costly and, particularly if their cost is greater than the losses they are intended to prevent, they are therefore not likely to be acceptable for general use. Therefore it may also be appropriate for the carriers to place before the Commission relevant cost and current fraudulent loss data as well as purely technological data. Naturally, all of this type of sensitive information must be protected from view by the general public, by competitors and possibly also, in certain cases, by the adversaries in the hearings, via a suitable sealed submission procedure so the sensitive information is examined only by the Commission staff.

As a non-attorney speaking to a group of legally experienced readers, I recognize that I may well be "reinventing the wheel" with regard to these conclusions about procedural and evidentiary topics. However, from my own technological and non-legal point of view, this docket appears to be particularly heavily clogged with non-issues which have been elevated to the status of issues due to the lack of necessary correct factual information or data, and a large amount of paper and time could have been saved if all parties were obligated to only present technologically substantiateable or substantiated data.

Comments on MUSDN: This carrier service is so intertwined with the issue of emulated extensions and the various objections to it that it requires special comment.

MUSDN is actually <u>not</u> a cellular network technology. It is just two separate cellular telephone sets which have their MIN value set to the same number. The two billing data records are merged in the billing process (in some cases by means of a secondary "off-line" billing software system) to present a single bill to the customer. In fact, as mentioned earlier, the fact that two MUSDN cellular phones have the same MIN but different ESN values is fundamentally incompatible with the North American IS-41 cellular network. Consequently, a MUSDN customer can only use the primary cellular phone while roaming. The second MUSDN phone will not work while roaming. Even if there are bad radio coverage areas in the home city of the MUSDN customer, the secondary MUSDN phone will not automatically switch over to the alternate carrier in that area (of course, assuming that the competitive alternate carrier <u>does</u> have adequate radio coverage in that particular area of the city, which in fact is often the case) as an ordinary cellular phone or an emulated extension or the primary MUSDN phone will do. This problem with MUSDN sets is not impossible to overcome by means of a "wholesale reworking" of the North American cellular network, but this will be a long term and very costly development process, particularly costly in view of the relatively small market penetration of MUSDN. Emulated extensions have none of these shortcomings, since either set will work both at home and when roaming, using the alternate carrier, etc.

Both emulated extension phones and MUSDN phones have the limitation that they cannot be powered up simultaneously, because they will both respond to paging messages (paging messages use only the MIN – not ESN -- to locate the cellular phone) and produce other simultaneous or near-simultaneous messages to the cellular network on the setup channel, such as autonomous registrations, etc. At present the call processing treatment is uniform for all makers of MSCs. Only one of the two (or more) sets with the same MIN (whether MUSDN or emulated extension) can have a cellular call at a given time. Once one set is engaged in a connection, the other one cannot begin or answer a call. This could also be change by means of new software development, but first there must be a definition of what the desired behavior of two such sets should be, which is accepted by the industry and approved by an appropriate standards committee. I must emphasize that this applies equally to both MUSDN and to emulated extension sets.

Both emulated extension and MUSDN cellular phones (if both sets with the same MIN are improperly left in a power-on condition simultaneously) are able to cause certain problems to the cellular network and to the "velocity" or "time

place" anti-fraud methods. AWS, CTIA and other carrier petitioners have repeatedly claimed that customers will not be able to properly prevent the simultaneous power up condition of multiple emulated extensions, but at the same time, they do not give any credible reason (or in fact any reason) why MUSDN customers would not be equally likely to leave multiple sets in a power-on condition just as often as emulated extension owners. Rather than just argue endlessly about this issue, I would like to propose that some substantiating data be put forward on this topic, and if it is not forthcoming, I suggest that the allegation of extraordinary simultaneous unwanted setup channel signals no longer be considered in these deliberations. To produce substantiating data, first, the carriers are in a unique position to present real data from the so-called "stats" produced in the normal course of business by the MSCs under their control. They can present the actual counts on the number of occasions in which MUSDN customers have improperly left multiple MUSDN cellular phones (which they can already unambiguously identify) powered-on simultaneously, thus leading to simultaneous paging responses, autonomous registration messages, and the like. The data should be drawn from a number of different markets and cells in a number of different calendar months in accordance with good statistical sampling criteria. This data can be compared to the number of MUSDN customers in each such market to determine the rate of such mistakes by MUSDN customers (the rate being the ratio of the number of erroneous messages per month per MUSDN cellular phone). It appears to me that this number is a reasonable basis for extrapolation to determine how often to expect similar errors by emulated extension users as well. If the carriers have good reasons to present which would indicate that the expected rate for MUSDN users is different from emulated extension users, let them present their reasons and let the Commission evaluate them. If there is a concern that the carriers would be releasing proprietary competitive information in this form, let them present this data only to the Commission and not to their adversaries in the hearings. I trust that this will put the discussion on a quantitative and factual basis, rather than continuing on the basis of repeated qualitative accusations, rebuttal, acceptance of the correctness of the rebuttal, and then the same accusation repeated all over again.

13. **Recommendations**: My recommendations in this section are merely an abbreviated summary of a few of the many specific proposed revisions with comments and explanations contained in the previously noted August 10, 1995 letter (and its attached exhibits) from Tim Fitzgibbon to Regina M. Keeney of the Commission, highlighting only those portions which bear on the specific points in the previous rebuttals of this letter. I earnestly refer the interested reader to Fitzgibbon's letter for more details and explanation. Regarding the specific subject of Rule 22.919, I suggest that the Commission modify that rule to address the following considerations:

13.a A general prohibition on modification of the ESN should be so worded that each mobile station should be manufactured with a unique ESN value, and any modification which makes the cellular set *capable of transmitting* an ESN value different from that set by the manufacturer is prohibited (with only the following specific 3 classes of exemptions: d, e and f below), rather than a narrow prohibition which only prohibits changing the ESN value in memory.

Comment: Wording which only prohibits changing the ESN in memory will give a criminal a loophole to evade conviction, by use of a mobile station which has been modified in such a convoluted manner that the original ESN is untouched and still resident in the proper memory location, but a knowledgeable criminal user can cause the set to selectively emit a different unauthorized ESN value. That emission is what allows the cellular phone to identify falsely for purposes of billing fraud, not the nominal value of ESN in the memory.

It is also desirable that coordinated steps be taken in other areas of the law to, for example, possibly make import, or possession (in addition to use) of a set which does not meet the provisions of this rule, and its explicit exceptions, an offense. Rules prohibiting monitoring the setup or voice/traffic channels to "harvest" of ESN values off the air for fraudulent purposes are also desirable, although they have no logical connection with the way a cellular phone transmits its ESN value or Rule 22.919. Such additional laws are clearly beyond the scope of this Docket, but would be significant in a properly organized legal program to apprehend and prosecute criminals.

13.b I strongly recommend that the Commission rules do not mandate encoding or splitting the ESN in memory in any particular way, or splitting the ESN into non-contiguous pieces in the cellular phone memory. Crooks know how to defeat this, by running a "program trace" on one sample set of the same manufactured type, and after that there is no secret anymore, and there is no protection afforded by special coding or splitting. Leave the implementation details of how the ESN is stored in the cellular phone to the design discretion of individual manufacturers.

13.c Authentication according to the TIA standard should be a requirement, as soon as it is feasible, for all new type approved sets for 800 MHz band cellular service. Authentication, even in a "one-piece" implementation, is so much more secure than use of a non-authenticating set that it should be mandatory because of its value to the industry. Because a "one-piece" implementation of authentication is easy to add to the software/firmware of a design already frozen in hardware form, it should be permitted, but nothing in the wording should prohibit the use of the even more secure separable chip implementation.

Comment: In addition to the specific measures mandated immediately by proper wording of the rule, as noted in the previous paragraph, I also suggest that the Commission should take all appropriate steps to encourage and promote the use of the most secure separable chip implementation of the authentication standard. A working group with representatives from carriers, manufacturers, and consumers should confer with all affected parties to arrive at a practical yet early date for mandatory separable chip implementation of authentication, as well. As discussed in section 7.2, manufacturers will most likely make this secure implementation once it is mandated, rather than being left as a competitive issue with cost penalties to the innovators of fully secure cellular phones.

In addition, to fill in the remaining gap, I most strongly recommend that, as soon as it is feasible (after consultation with the parties noted above), the Commission mandate by means of a further future addition to Rule 22.919, that then current ongoing manufacture of all cellular sets which have been previously type approved are manufactured only with authentication incorporated at the factory. Exemptions could be given for only those types of sets which the manufacturer can show are technologically incompatible with such an upgrade. However, I frankly do not expect to find any current production cellular phones which are incompatible with an authentication upgrade. Since authentication requires some additional non-volatile memory for such data as the A-key, SSD-A, etc., it is possible that such an upgrade in some cases will reduce the number of memory locations available for such features as stored speed-dialing numbers or other non-authentication related features. If only non-essential features like this are slightly reduced in this way, this alone should not be an acceptable reason to exempt a set type from being upgraded for authentication in continued manufacture.

13.d Three specific classes of exemptions from the general prohibition on changing the ESN are desirable now:

13.d.1 An exemption for the case of a separable chip implementation of the authentication algorithm, which chip incorporates the ESN and which is designed by the manufacturer to be moved from set to set. In this case, there should be no explicit or implicit prohibition on possession and use, by a single valid cellular customer, of multiple cellular sets and/or chips having the same MIN/ESN/A-key and related authentication data, but I agree with the comments of several others that a reasonable limit on the number of such emulated extensions should be mandated by the commission for administrative convenience I believe that the limit on landline extensions in part 68 on a single subscriber line is 12, as a starting point for discussion.

Comment: Note that the legal permission for such a move or copy of the identification incorporates the case of a chip on a chip carrier, or a chip packaged in a "smart card." The special case of replacement of a non-functioning set of this type is covered by removing the chip or smart card from the old to the new set. This changeout of the separable authentication chip is the standard procedure used in the European GSM system for the purposes of repair and upgrade, and also for rental of a cellular set for a short term, use of a semi-public GSM cellular radio in a taxicab, etc. Note that in this implementation the ESN is now in the chip and does not remain in the cellular set, unlike earlier technology and unlike paragraph 13.d.2.

It is also desirable, for a cellular phone having authentication, and particularly when the ESN is in a separable chip and not in the remaining portion of the cellular phone, to mandate a separate unique physical equipment identifier, distinct from the ESN. I suggest a physical equipment identifier, initially installed in the cellular phone's non-volatile memory at the factory, which can be remotely determined over the radio by the cellular network via a special interrogation message, because this is already done successfully in the European GSM system. However, the industry standards committees should determine the final form of this particular identifier, since other methods have value as well. This physical equipment identifier is not in the separable chip. It is not desirable to unconditionally prohibit changing this physical equipment identifier, since changing it facilitates repair and upgrading, and in any case it has absolutely no relationship to authentication or fraud. It is important for tracking stolen cellular phones or repair-related identification, so its alteration in connection with theft or unauthorized use of a cellular phone should be prohibited. However, if a manufacturer or a third party upgrades the software in the cellular phone legitimately, this is a desirable instance to change the physical equipment identification number to allow systems to automatically determine the capabilities of the cellular phone from its physical equipment identifier, which has a number of network-wide benefits.

13.d.2 An exemption for a phone in which there is no separable chip authentication but instead a "one-piece" call processing and authentication implementation, or a phone in which there is call processing but no initial factory provided authentication, and when all of such sets involved in the transfer or copying of the ESN are owned by the same valid cellular customer, and one of these retains its original ESN value. As in the previous paragraph, there should be no explicit or implicit prohibition on possession and use of multiple cellular sets having the same MIN/ESN by a single valid cellular customer, with some maximum set by the Commission. Note that this exemption also covers changing the ESN of a set to repair, replace or upgrade it, and this should be explicitly mentioned in Rule 22.919. In addition to changing the ESN in a secondary cellular phone to match the customer's primary phone for use as an extension, the Commission should explicitly recognize the changing of the ESN in the customer's cellular

phone when that customer is the victim of cloning, but wishes to retain the original directory number (MIN) and change the phone's ESN only.

Comment: I agree with several petitioners that the commission should establish appropriate procedures to control who is permitted to do this type of change (the so-called "emulators") and under what conditions what type of records are kept, and to define the responsibilities of such emulators.

The particular acceptable technological methods for changing and controlling propagation of the ESN in this case (e.g. encrypted transfer, erase-before-write, central data base, etc.) and the responsibilities of persons and firms engaging in such operations (e.g., identification of who is permitted to make such changes in ESN, maintaining a central data base to prevent duplicate ESN values from being assigned, copying the ESN from a non-functioning set to a good set for use by the same valid cellular customer, etc.) should be specified.

In addition, I most strongly recommend that as soon as it is feasible, all sets which have their ESN changed in this way are also mandated to have authentication software added as well. Some reasonable calendar target should be set to allow for development and testing of the upgrade software. Specific types of sets could be exempted only if authentication is already installed, or if the manufacturer can show that the set is technologically incompatible with such an upgrade, or if the manufacturer makes such an upgrade available directly at a reasonable and competitive cost to the customer in the case that the manufacturer chooses to restrict the alteration of the software by others as a result of copyright or other special rights to the software. No manufacturer should be permitted to restrict or prevent authentication upgrade of upgradeable sets by asserting copyright or other legal rights, unless they make such a software/firmware authentication upgrade available directly to the consumer at reasonable and competitive cost. The Commission should also consider a completely separate rule mandating that any cellular phone which is repaired for any reason must also have authentication added as well.

As in section 13.d.1, a separate physical equipment identifier is desirable for theft tracking or repair related identification, and the rule should mandate installing such a number, and the software to permit remotely reading it. This same rule should apply equally to both emulated extension phones and MUSDN extension phones as well. (See comments above at the end of section 2)

13.d.3 An exemption for cellular band equipment such as BellSouth Cellemetry ®, in which the value of the ESN is changed solely to report remote measurement data, provided that the possession and use of such a cellular phone is restricted to a valid cellular customer and the cellular phone is not manufactured nor modified so that it is capable of transmitting via or utilizing a voice or traffic channel.

Oath: I declare under penalty of perjury that the facts set forth in this letter are true according to the best of my knowledge, information and belief.

Respectfully submitted,

Richard C. Levine

Original to Ms. Michele Farquhar, FCC
7 copies to Secretary of FCC
Copies to petitioners: AT&T Wireless Systems;
CTIA; MT Communications.

Attachment: Appendix A- BellSouth Cellemetry (4 pages)®

Cellemetry℠

Thomas F. Evans

Network Access Strategy
BellSouth Wireless, Inc.
1100 Peachtree Street NE, Room 808
Atlanta, Georgia 30309

Abstract

Cellemetry℠ provides the means of collecting, sorting and routing short telemetry-like messages via the standard cellular telephone system. At no time does the Cellemetry℠ system impose any significant capacity restraints on the cellular telephone system.

Cellemetry℠ is applicable to a myriad of business requirements, literally any business which requires one-way or two-way short message capabilities, such as utility meter reading, alarm panel reporting, vending machine status reporting, etc. Cellemetry℠ provides an inexpensive means to obtain information which heretofore was obtained by manual device reading or simply was not gathered at all.

Cellemetry℠ uses the overhead control channels on the cellular telephone system to convey its messages in either direction. The overhead control channels are used to deliver all of the messages between the cellular telephone base station and the customer's cellular telephone. These messages are required to initiate cellular calls and maintain contact with the cellular telephones. The message handling capability of these control channels is far greater than is needed to maintain the cellular telephone call traffic, even in the busiest of times during the day. Cellemetry℠ makes use of this excess control channel capacity to route its messages.

Cellemetry℠ RADios (CRADs) imitate cellular roamer telephones. A roamer telephone is defined as one which is operating outside of its home cellular system. Each cellular system sends a message at regular intervals to all of the roamers operating in its system, telling them how to operate as a roamer. One of the requirements as a roamer is to autonomously register (AR), during which time the cellular telephone reports its mobile identity number (MIN) and electronic serial number (ESN) to the cellular system via the Reverse Control Channel. The cellular system processes this MIN and ESN and routes them via a special network back to the cellular customer's home cellular system which validates the customer's identity and provides all of the customer's calling features. This action is an effort to reduce fraudulent calls as well as provide full calling capabilities even when a customer is roaming. The Cellemetry℠ gateway is connected to this intra-system network and since all of the Cellemetry℠ MINs will be specially assigned, the Cellemetry messages are routed only to the Cellemetry℠ gateway.

The Cellemetry℠ gateway processes the Cellemetry℠ messages according to their type. Some are processed immediately and passed on to the customer (alarm monitoring), while others are stored and delivered to the customer in a batch (utility meter reading). The gateway also handles billing for the Cellemetry℠ service.

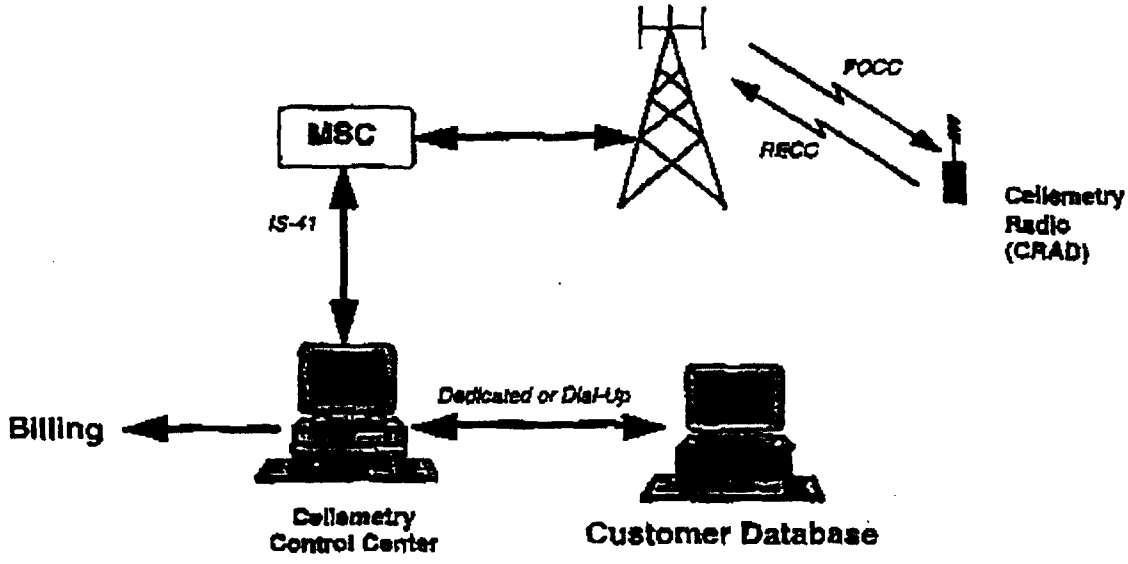


Figure 1. Cellemetry℠ Architecture.

Two data elements which are conveyed via the control channels are the Mobile Identity Number, or MIN, and the Electronic Serial Number, or ESN. Cellemetry℠ uses the MIN as an account or unit identifier. The MIN is ten digits long, the same as a standard telephone number plus Area Code. The ESN is a 32 bit number which can yield over 4 billion combinations. It is the ESN which carries the Cellemetry data message. The CRAD has the capability to store a number of MINs other than its main account identifier MIN. The action that the CRAD takes depends upon the register location in the CRAD's memory of each MIN. This action will be described in detail later.

Each CRAD acts like a roamer cellular telephone to the cellular system. A roamer cellular telephone is defined as any cellular telephone operating outside of its home system. When a cellular telephone is first activated, a Station IDentity, or SID, is programmed into the telephone. Each time the telephone is turned on, the telephone compares the SID stored in its memory to the SID transmitted by the cellular operator over the FOCC. If a match occurs, indicating the customer is in their home system, nothing happens. If a match does not occur, the telephone illuminates its "ROAM" light to indicate to the customer that they are not in their home system and that roaming charges will apply to their telephone calls. Little else occurs to the cellular telephone. However, the telephone call from a roamer is treated very differently in the cellular system. It is this difference that is used to properly route the Cellemetry℠ message.

Since a cellular telephone system does not have any data on a roamer, such as whether they are a legitimate customer and have paid their bill, the cellular telephone systems have an interconnected network, called the IS-41, over which one cellular system can request information on a roamer from the roamer's home system. The home system replies back with confirmation of the roamer's identity, payment status and any custom calling features that the roamer has in its home system. The MIN is used to route the request for the roamer information via the IS-41 network.

In the case of Cellemetry℠, the MIN of the Cellemetry℠ unit is such that the cellular switch routes the MIN and ESN of the Cellemetry user to a specific port of the IS-41 network. At this port, the Cellemetry℠ Gateway is connected. Typically, the Cellemetry℠ Gateway is physically located in

the busiest cell sites, there is more than enough capacity for Cellemetry℠. To further eliminate the possibility of having any impact on the cellular system, the CRAD utilizes the busy-idle bit which is sent over the FOCC. The busy-idle bit is one bit multiplexed in the FOCC data stream which indicates that the cellular base station is communicating with a cellular user. A cellular telephone will not attempt to register with the cellular base station if the busy-idle bit is set high. Only if it is set low will the cellular telephone attempt a registration. The CRAD looks at the busy-idle bit over a multi-second window. If the busy-idle bit is set high for greater than a certain percentage of the time, the CRAD will defer its registration until the busy-idle bit activity is reduced. In this manner, regular cellular customers always will obtain the control channel first.

IV. Summary

Cellemetry℠ provides for an efficient, low-cost short message service which covers the entire footprint of a cellular system with no additional equipment required at the individual cellular base station sites. It can be easily and quickly installed with no impact on the capacity of the host cellular system.

Attachment 7

Wireless Telecommunications Bureau

Cellular Frequently Asked Questions

1. Does the FCC regulate or approve tower locations for cellular companies? How do I get a list of all cellular tower sites? Does the FCC have this information ?

Answer:
No. This is a local matter that is handled by state and local zoning boards. The new Telecommunications Act instructs the Commission to insure that the state and local zoning boards do not unreasonably delay the construction of towers or the approval of sites. More information concerning tower siting is contained at this link.

The FCC does not maintain a data base with all cellular cell sites. The FCC only maintains a data base of the external cell sites of each cellular system. These are the cell sites whose contours make up the outer boundary of the cellular system. These external cell sites are listed on the authorization for each cellular system.

You may review or make copies of cellular authorizations in the Public Reference Room of the Wireless Telecommunications Bureau's Commercial Wireless Division which is located on the fifth floor of 025 M Street, NW, Washington DC 20554, telephone (202) 418-1350. On-line dababase searches can also be accomplished in the Public Reference Room.

The FCC does not duplicate these records, but has contracted with International Transcription Service, Inc. to provide this service. Requests for copies of information should be addressed to International Transcription Service, Inc. (ITS, Inc.) 2100 M St., NW, Suite 140, Washington, DC 20037, Telephone (202) 857-3800.

2. Can a subscriber have multiple phones with the same telephone number?

Answer:
Yes, but there are restrictions. Each individual phone must have a unique Electronic Serial Number (ESN). The ESN is a unique number programmed into each cellular telephone at the time it is manufactured and is the means by which a cellular carrier identifies a telephone to determine whether the user of that phone is entitled to obtain service and to insure that the proper accounting is made of all activity. Most cellular phone emulators or extension services simply "clone" cellular phones, duplicating not only the telephone number but also the ESN. This activity is in violation of current Commission rules.

The Code of Federal Regulations Title 47, Section 22.915, entitled Cellular System Compatibility Specifications, generally sets forth the standards of cellular operation as reflected in the Cellular System Mobile Station-Land Station Compatibility Specification (April 1981 ed.), Appendix D to the Report and Order in CC Docket No. 79-318, 86 FCC 2d 469, 567 (1981). It is a violation of Section 22.915 of the Commission's rules for an individual orcompany to alter or copy the ESN of a cellular telephone so that

the telephone emulates the ESN of any other cellular telephone. Moreover, it is a violation of the Commission's rules to operate a cellular telephone that contains an altered or copied ESN.

Part 22 of the Commission's rules was recently revised to add a new rule Section 22.919, to further clarify the issue of ESNs. Pursuant to subpart (c) of the referenced section, it is a violation to remove, tamper with, or change the ESN chip, its logic system, or firmware originally programmed by the manufacturer.

It currently is possible to obtain two cellular phones with the same telephone number if the cellular carrier in the market has the software in place to handle the billing and its fraud detection system has been notified not to be triggered by the use of two phones with the same phone number in suspicious circumstances.

---

3. How do I get a cellular license?

Answer:
The Commission divided the United States up into 734 different markets where it licensed two entities for each market. The largest 306 markets are Metropolitan Statistical Areas (MSAs) and the remaining 428 markets are smaller Rural Service Areas (RSAs). The majority of these markets have been licensed and all that remains to possibly be licensed is what the Commission has defined as "unserved area". Each of the MSA and RSA licensees was provided five years to build out their systems within their designated market area. At the end of the five year buildout period, licensees are required to notify the Commission of what area they actually cover within the market area. This covered market area is called their Cellular Geographic Service Area or CGSA. Any area within their MSA or RSA that is not their CGSA or covered service area after five years is available for unserved area licensing. The unserved area licensing process is two-fold.

Phase I is a one-time process that provides an opportunity for eligible parties to file competing applications for authority to operate a new cellular system in, or to expand an existing cellular system into, unserved areas as soon as these new areas become available. Phase I initial applications must be filed on the 31st day after the expiration of the five year build-out period of the authorized system(s) on the channel block requested in the market containing the unserved area. Each Phase I application must request authorization for one and only one CGSA in one and only one cellular market. Additionally, each licensee whose Phase I initial application is granted is afforded one opportunity during the Phase I process to file an application proposing major modifications to the cellular system authorized by that grant, without being subject to competing applications.

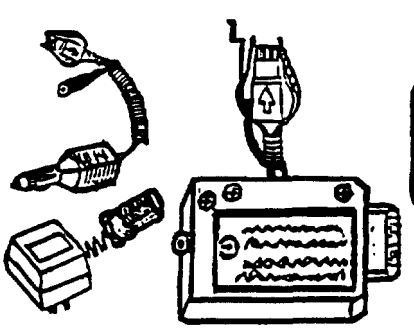
Phase II is an ongoing filing process that allows eligible parties to apply for any unserved areas that may remain in a market after the Phase I process is complete. If a Phase I initial application is granted for a market and channel block, Phase II applications (applications for authority to operate a cellular system in any remaining unserved area) for that market and channel block may be filed on or after the 121st day after the Phase I application was granted. If no Phase I initial applications are granted for a market and channel block, Phase II applications for that market and channel block may be filed on or after the 31st day after the FCC dismissed the last pending Phase I application. If no Phase I initial applications are received for a market and channel block, Phase II applications for that market and channel block may be filed on or after the 32nd day after the expiration of the relevant five year build-out period. There is no limit to the number of Phase II applications that may be granted on each channel block in each market

FCC

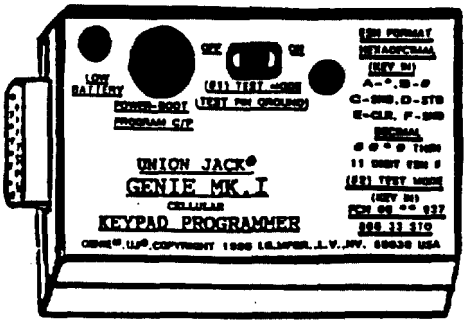
Attachment 8

NEW FOR 97!

GENIE MK-1 KEYPAD ESN PROGRAMMER



DIM:1 1/2 X 1" X 1/2"



DIM:3 1/4"X 2 1/4"X 1"

NOW
$799

PROGRAMS
FIRMWARES
9123 TO 96C1
EE-3 !
EE-1 & 2

UJ's Genie Mark I Keypad Programmer is a fully mobile,ESN programmer for Motorola Flip Pocket Cellular Phones. After connecting to the phone's 8 pin data port, it utilizes the Phones keypad ,LED Display and battery to program ESN numbers with firmwares up to 961C. this includes EE1, EE-2 & EE3 phones.The Genie itself is powered by a 9V rechargeable battery, & is small enough to fit into your shirt pocket.The ESN is entered in hex-format by using the "*" key for A, "#" for B, "RCL" for C, "STO" for D, "CLR" for E & "SND for D or Decimal format, enter # # * #, then the 11 Digit Decimal ESN number. (No calculator necessary. Most EE-2,EE-3 phones ESN change is done in 30 seconds, others 1 minute. The included connecting cable is a specially modified one-piece genuine Motorola data cable with built in battery center pin and it's opposite end has a DB-15 plug with battery charger jack (DB-15 plugs into the Genie.)The Genie systems has no dangling wires, fully portable,self contained and is upgradeable to other Motorola, Etc., Manufacturer's Cellular Phone, as available. Warranty 1 year. GENIE MK-1 SET $899.

Genie Mark II Keypad ESN Programmer

The Genie Mark II Keypad Programmer contains all the features of the Mark I except it is desighned to also program all Motorola Elite and Star Tac phones. It will include 3 different cable sets for connecting to the Flip-Pocket phone's 8 pin data port. The Elites 10 pin data port and Star Tacs 15 pin port. The Genie Mark II will be available late 97.

NOTICE

Genie's I/O, VCC circuits are Schottky Diode/R protected against ESD/NVC/T (per Dallas Semiconductor's Apllication Note #AN-93, 053095),includes 1 year limitted warranty with technical backup and is Manufactured in USA.

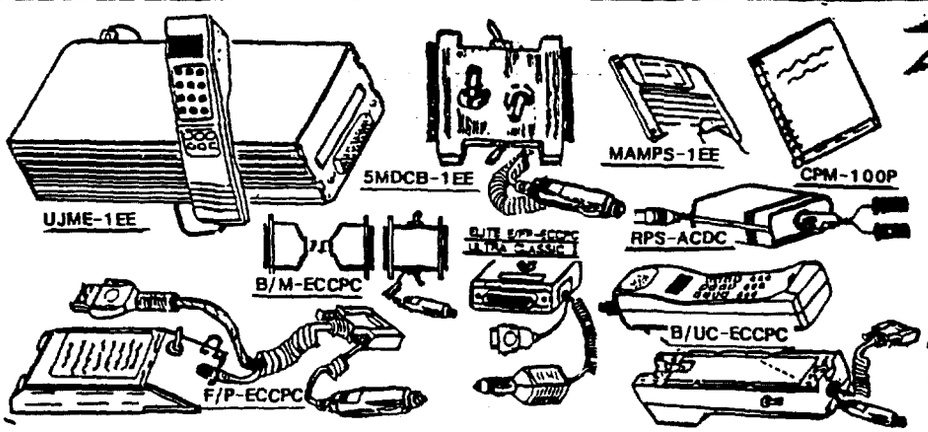
GENIE MARK I INCLUDES

1 each 8 pin Data Port- Motorola compatible Interface cable set assembled with DB-15 plug & Genie Ni-Cad Battery charger Jack. 1 each Genie 9V Ni-Cad battery and 1 each modified 6.5V Motorola type Flip-Pocket Cellular Phone's Battery.1each combination Dual Voltage automatic Ni-Cad Battery Charger (INPUT 12.VDC) (Output 9VDC for Genie-6.5V for Cellular phones battery), 1each AC to 12.5VDC output Power Adapter Transformer.1 Set Genie's operating instructions,1 each UJ's 100 page Cellular Technicians Programming manual, QUICK TECHNICAL BACKUP SERVICE and Electrical-Mechanical Warranty.

UJ'S COMBO SALE

BASIC EMULATOR SET, NOW!

COMBO A NOW $249!



COMBO B NOW $298!

COMBO C NOW $348!

COMBO(A): INCLUDES L/R EMULATOR, PROGRAMING INTERFACE CONTROL BOX, SOFTWARE, REGULATED AC TO DC POWER SUPPLY & 100 PAGE CELLULAR PROGRAMMER'S MANUAL.

COMBO (B): $298 INCLUDES ALL ITEMS COMBO (A), WITH YOUR CHOICE OF 1 EACH INTERFACE CABLE HARDWARE SET.

COMBO (C); $348 INCLUDES ALL ITEMS COMBO (A), WITH YOUR CHOICE OF 2 EACH INTERFACE CABLE HARDWARE SETS.

EMULATOR SYSTEM, COMBO A

UJ'S®, EMULATOR-TEST INSTRUMENT. (REFURBISHED-DEACTIVATED-MODIFIED CELLULAR PHONE) EFFORTLESS 5 STEP, 5 MIINUTE PROGRAMMING, (FOR COMMERCIAL USE). UJ'S EMULATOR SYSTEM EXTENDS MOST POPULAR MOTOROLA SOFTWARE, PROGRAMS FIRMWARES TO 9525/.REPAIRS 0000FFFFS. UJME-1EE EMULATOR SYSTEM C O M B O A. includes (A) Emulator UJMEE-1EE, (B) 5 mode 5MDCB-1EE emulator control box, (C) Motorola's 212 page, Cellular Technicians Traning manual (D) SOFTWARE: MAMPS-1EE MOTO-EMULATOR-G2EE programs for AMPS-NAMPS-ETAC SYSTEMS TO FIRMWARE 9525,. (E) 117 VAC to 12.5V DC power adapter, comprehensive UJ'S instructions with LATEST SCHEMATIC DIAGRAMS FOR CONSTRUCTING YOUR OWN MOTOROLA INTERFACE CABLE SETS & most important, TECHNICAL BACK-UP! SAVE$100, C O M B O A OFFER $394.95. S E P E R A T E L Y: * (A) UJME-1EE EMULATOR ONLY WITH AC/DC POWER ADAPTER $249.95, (B) 5MDCB-1EE 5 MODE EMULATOR DATA CONTROL BOX $149.95 (C) MOTOROLA CELLULAR TECHNICIANS TRAINING MANUAL $45.00 (D) MAMPS-1EE SOFTWARE SET WITH G2EE $99 & (E) PAE-1EE EMULATOR AC TO DC POWER ADAPTER $9.95.
WARRANTY: ALL ITEMS INCLUDE UJ'S 6 MONTH ELECTRO-MECHANICAL WARRANTY.
ORDER INFORMATION: S&H $25.00 PER ORDER VIA FEDEX.
PAYMENT METHODS: PREPAYMENT ONLY BY WESTERN UNION (QUICK COLLECT) OR USA POSTAL MONEY ORDER VIA FED EX, DEDUCT $10 FROM TOTAL ORDER AMOUNT).
FREE CATALOG-TECHNICAL BACKUP ETC: TELEPHONE 702-642-0325 OR FAX 702-642-3558

"OUR 4TH YEAR SALES, NUTS & VOLTS, 99.5% SATISFIED CUSTOMERS!"
LESS BUSTER'S ELECTRONICS 2039 CIVIC CENTER DRIVE #176 N. LAS VEGAS, NV 89030.

SUMMARY OF EMULATOR'S OPERATION

The original phone is properly connected to the Emulator. Both their adapter's switches are placed in the proper positions & both devices are powered up from their keypad's. The transfer commands are entered on both keypads. The Emulator handset will display "PASS". What is happening during the transfer process, is a swap of the ESN/NAM data between these devices. The "FFFFFFFF" ESN & NAM data from Emulator will now be in the Original phone whatever ESN/NAM data that was in the original phone will now be Emulator. The Emulator is connected via the parallel port to a IBM compatible Computer & the MAMPS-1EE program is used to edit the ESN/NAM data that is tempórarily stored in the Emulator. After editing of the data in Emulator is completed, we again connect the original phone to the emulator & the keypad commands are reversed, when completed properly, "PASS" will now be displayed on the original phone. The edited data from Emulator will now be in original the phone & the FFFFFFFF ESN will be back in the Emulator.

COPY CAT

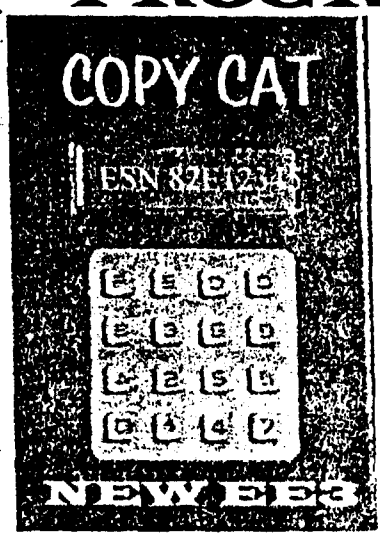
NEW STARTAC Soft ware

7 way EE3/9611 Soft ware

$195.00

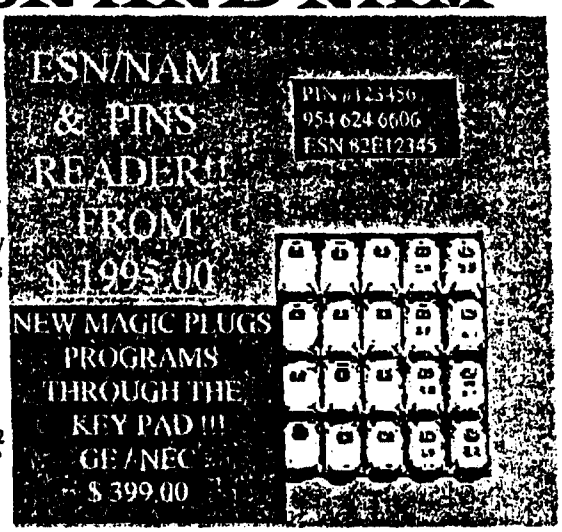
ANY QUESTIONS

PROGRAM ESN AND NAM



1 MOTOROLLA, EE3 / 9611
EE2 / 951C /
9449 /BRICKS:
Flips,ELITES,ULTRA
CLASSICS,ULTRA
CLASSICS 2, CARPHONES
ANALOG&DIGITAL.
2 AUDIOBOX: Audiobox 500 &
700 &800.850
3 G.E./ERICSONS: OLD / NEW
G.E. 700 ,550,500& G.E. Flips
4 MITSUBISHI/DIMATEL
3500 & 4000.
5 NEC P200/P300/P400/P600
P110/P120/P180/P700
ALL HANDHELDS !
6 SONY:333
7 PANASONIC 3531,3551,3552

COMPLETE SET OF MOTOROLA CABLES (FLIP, BRICKS ULTRA-CLASSICS, $225.00



AAA CELLULAR(954) 923 3518

12864 BISCAYNE BLUD 264 NORTH MIAMI FL 33181

AMAZING PROGRAM. You teach it linear related subjects by example to solve a wide variety of word problems. No formulas or equations required. Create text for word problems such as **MILES TRAVELED at 65 MPH** and **DESTINATION HRS.** For the above word problem you would then give the program two intuitive examples of miles with related hours answers, like (65 miles is equiv. to 1 hour and 650 miles is equiv. 10 hours). You can then enter new values for miles to travel at 65 mph and the program will display time to destination answers. The program can also print a list of answers for a selected range. Learned subjects can be saved and recalled. Build your own expert subject base. PC, VGA, 3-1/2" 1.44MB drive. Send $20.50 plus $4.50 S&H by check or money order to: INVOTEK Dept.: CONVERT-IT, 2910 East 16th St., Muncie, IN 47302.

SHAREWARE CATALOG. Over 3,000 programs, free game on every catalog disk. Great prices, bonuses, free disks. Data Mate, Box 2811, Ronkonkoma, NY 11779.

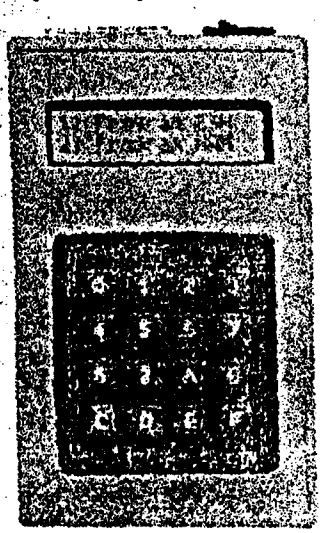
coupon! Inexpensive, quality, IBM Shareware and CD-ROMS. <ASP> vendor: **MOM 'N' POP'S SOFTWARE.** PO Box 15003-N, Springhill, FL 34609-0111. 352-688-9108.

IBM SHAREWARE. Free catalog, $1 disk, 35¢ specials, huge selection, 100% virus free. PMA, Box 2424, Scottsdale, AZ 85252. 602-496-6547. Specify disk size.

I WANT it and I want it now. I want all of your SIMM memory. IBM, Mac, new, used, even defective. I want it all. Highest $ paid. Now selling memory. We can beat any printed price in Nuts & Volts. Call 1-800-4-MEMORY now! Voice/FAX.

LINUX! LINUX! LINUX! If you aren't purchasing your Linux products from us, you are paying too much! We offer the major distributions (Yggdrasil, Slackware, Red Hat, etc) at **great prices!** We also carry a full range of books. Contact us at **www.cheapbytes.com** and use our secured web server. E-Mail: sales@cheapbytes.com Fax: 209-367-8518. Cheap*Bytes, PO Box 2714, Lodi, CA 95241.

CopyCat



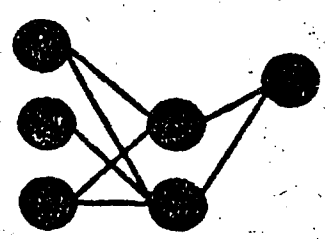
Motorola Boxes Starting At
$1495

Now Available:
***EE3**

- *Pocket Size
- *Operates on 9-volt Battery
- *Easy to read LCD Display
- *7-Way Boxes
- *Load Code Removal
- *Repair & Update Old Units

"CopyCat, Black Box, Stand-alone Programmer"
You have all heard of this amazing device, now you can own one for yourself. Complete with cables, and easy instructions. No kit to put together. Completely Assembled & Pre-tested.
Electronic Service & Supplies
219-744-4788
BYDN38B@Prodigy.com
http://www.cris.com/~macguyvr

Write In 155 on Reader Service Card.



NEURAL LAB with basic source code library $29.95. "C" source code library $29.95. Includes pattern recognition and speech recognition examples. We also have many more AI and robotics items! Zagros Software, PO Box 460342, St. Louis, MO 63146-7342. 314-768-1328.

http://www.hackerscatalog.com Telecode's "Hackers Catalog" is now online. Everything the catalog contains and more. You ain't surfed yet!

18,000+ TECHNICAL REPAIRS for TVs, VCRs, PROJECTION TVs, CAMCORDERs, AUDIO on disk. Installs on your hard drive. Easy look-up by model/chassis number. For **DEMO version send $10 to: HIGHER INTELLIGENCE SOFTWARE, 60 FARMINGTON LANE, MELVILLE, NY 11747. $10 is refundable** toward purchase of the regular version of the TIP PROGRAM. **1-800-215-5081/516-643-7740.**

CP/M SOFTWARE, also Amstrad PCW software and hardware. 3", 8", and hard sectored disks. Disk copying, 400 formats. Send $2 for catalog, SASE for FREE flyer. Specify computer. Elliam Associates, PO Box 2664, Atascadero, CA 93422. 805-466-8440.

THE RELIABLE bulletin board service, software for all needs. Call 718 area code USA: 987-1932, 987-2913, 987-1617, 987-1660.

Civic Center. 770-907-6225

NOVEMBER 30

IL - LITCHFIELD - Amateur TV Club Banquet. Ariston Restaurant. Scott Millick 217-532-3837
IN - EVANSVILLE - Winter Hamfest. Vanderburgh Co. Fairgrounds. Neil 812-479-5741

NOVEMBER 30-DECEMBER 1

NJ - PENNSAUKEN - Computer Show. South Jersey Expo Center. KGP Productions 908-297-2526
OH - COLUMBUS - Computer Fair. Veterans Memorial. Mark Hanslip 513-263-3378

DECEMBER 1996

DECEMBER 1

Black B.B.	$195	Pio 5100s	$[illegible]5
FC's	$215	03-VI	$175
Z MANN 1600s	$135	Black-S 35s or 50s	$135

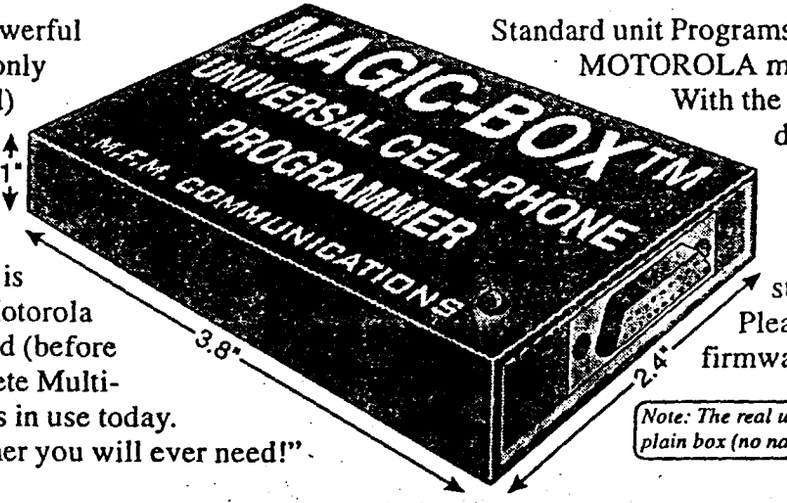
CALL 1-800-945-6625

ANYONE IMPLYING THEFT OF SERVICE WILL BE DENIED PURCHASE.

"The Most Advanced Universal Cell-Phone Programmer"

"The MAGIC-BOX™ - Does Most Makes & Models via the Phones Keypad (much better than a Copy-Cat)"

The MAGIC-BOX™ is a small and powerful Universal Cell-Phone Programmer. It only requires the phone and a lead (supplied) to program the phone using the phone's own keypad. With the MAGIC-BOX™ attached the ESN is simply entered on the phone's keypad and then after a few seconds the phone is programmed! It is supplied to do the Motorola models as standard, but can be upgraded (before and after purchase) to become a complete Multi-Programming tool for almost all phones in use today. "This is the only Cell-Phone Programmer you will ever need!"



Standard unit Programs & Repairs (0000FFFF faults) all MOTOROLA models to 961C, (incl. EE1, 2 & 3). With the extra firmware upgrades it will also do all NEC, ERICSSON (incl. 96), MITSUBISHI, AUDIOVOX, STARTAK and much more!

Prices start from **only $999** for a standard unit and two lead sets. Please enquire for prices on additional firmware upgrades and extra leads.

Note: The real unit is a plain box (no name etc.)

Call Us Now on....
01144-188-333-0060

M.F.M. COMMUNICATIONS. 57 Addison Road, Caterham. CR3-5LU. UK.

"For Information Purposes Only"

Write In 40 on Reader Service Card.

...more great deals on used working equipment visit our Web site at: www.odulo.com/corp/equiptek 415-244-...

NEW, USED Hewlett Packard 10833A-D, HP-IB cables from $10. Call **Psitech Plus** 707-745-4804, fax 707-747-5277.

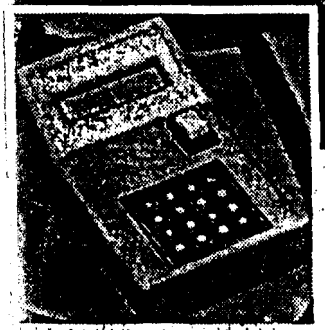
...also handle 478As and many others. Call or fax for more information. Willamette RF, Inc., 541-754-7226, FAX 541-753-4629.

...lar for used s... from HP, Tekt... at Metric for in... 3424.

S&N CELLULAR

The Electronics SuperStore

- Buy direct from the manufacturer
- 10 years of quality equipment & service
- The most competitive pricing in the industry
- Prompt delivery/Expert sales personnel



We offer a complete line of Cellular Progamming Equipment

"THE 951C KOPY KAT" - Program any Motorola phone - the Flip, the Micro-tac, the Ultra-Lite, the Elite, the 951C, or any installed or bag phone. Complete with all 4 cables, instructions, is battery operated for ease of use **$1695**

Sale Price

Motorola Loader Bag System - Programs up to 94 version, includes flip cable, computer cable and transfer box **$650**

NEC ESN Clip - Programs Model #'s 110, 120, 180, 181 .....**$600**

NEC ESN Clip - Programs Model #'s 400 & 600, ...**$600**

NEC ESN Clip - Programs Model #'s P700, P701, P760, P761 .....**$600**

GE, Ericsson ESN clip - Programs Model #'s **G.E.** CT700, CT550, CT750, CT800
Ericsson Model #'s AH210 AH220, AH235, AH237, AH238, AH300, AH310, AH320 ..**$500**

Mitsubishi, Diamond-Tel Software - Program Mitsubishi handheld Model #'s 3500, 4000, 4500 & newest 5000. Diamond-Tel handheld Model #'s 18X, 20X, 22X & newest 25X complete with cable, no phone disassembly required ...**$500**

OKI 900 - Programmable phone, modified
& complete **$600**
Chip installation only **$350**
Chip only - **$175**

NEW **C-TEK Cable** - Turn OKI 900 or At&T 3730 into a cellular monitor ...**$250**

* Call for Prices on Motorola EE3
* Call for Prices on Readers

Please call your courteous service representatives for complete details at:

(954) 974-6161

S&N Cellular • 934 University Drive, Suite 152 • Coral Springs, Florida 33071

AGREEMENT FOR PURCHASING OF CELLULAR PROGRAMMING SOFTWARE AND EQUIPMENT

...urchaser agrees not to use said software and equipment for any illegal purposes. This includes line fraud, computer fraud, cellular service fraud, ...nd any other fraudulent acts according to all federal and local laws, including rules of the FCC title #18, section 1029, and all Florida statutes. All ...oftware and equipment is sold only to qualified buyers. All software is sold for educational purposes ONLY!!!

HP 204C OS... synchronizes, $225, one, $1... VISA/MC.

MICROWAVE Watkins-Joh... **+10dBm** outp... frequency anc... $68,000; now... Hamilton Inst... 800-TO-BUY-T...

HP 3580A s... $1,000; HP 35... tive level me... 4436A attenua... 3465A, $200; ... $150; HP 480... 3490A, $300; ... Electronics 30...

POOR MAN'S Receiver Kit. ... $78. Now ava... filters, trackin... frequency reac... IBM compatit... envelope for d... 310B, Bethpag...

STEREO MIC dual magnifi... 10X&30X on ... $495. On dual ... 7-45X zoom ... available. Se... Redwood City. ... 415-365-5845

WAVETEK 1... Wavetek 157 ... $250; Wavetel ... $250. ISA, PO... 92607. 714-48... Mail: sklar@ce...

WANTED: L... **MENT** (Tektr... test equipmer... Systems, 214-...

COMMUNICA... **ER**, Polarad m... 10Hz resolutio... TTG-29 $600 ... 707-747-5277.

HP 8557A I... 350MHz spe... 8660B, HP 8... synthesized g... resolution, sw... 475 scope 20... 8640A (dial sc...

TEKTRONIX: 1433M $175, ... manual $150 ... Surplus, 714-8...

the best way to deter fraud. Customers can sign up for a PIN by contacting Bell Atlantic NYNEX Mobile customer service at 1-800-255-BELL, or calling *BAM toll-free on their cellular phone.

SIDEBAR #2:

BELL ATLANTIC NYNEX MOBILE'S WAR ON CELLULAR FRAUD

With a history of pioneering innovative anti-fraud technologies, BANM was the first wireless service provider to introduce the PIN system, making the cloning process more difficult. Last year, BANM reduced cloning fraud by more than 80 percent in its footprint by promoting use of the PIN. BANM's multi-tiered approach to fraud prevention also includes educational programs, new software systems, an in-house fraud task force, and other deterrents.

BANM also actively works with law enforcement officials to pursue criminal and civil action against cellular bandits. Last year, the company assisted law enforcement in making more than 300 arrests along the East Coast and has helped write and enact legislation making cloning a felony. Maryland's new law making cloning and the use of cloned phones a felony is an example of legislation that BANM actively supported. ###

that cloning fraud has dropped 90% from RF fingerprinting."

AT&T Wireless also has witnessed phenomenal results from the use of both authentication and RF fingerprinting. Last year, the carrier reduced fraud within the metropolitan New York area by 90%, bringing its overall fraud loss to its lowest point since 1991. It also has slashed the lifespan of a cloned phone to three days from a previous lifespan of 35 days to 40 days, and has decreased the number of customer-cloned phones by 75%.

> "RF fingerprinting and authentication provide a very good one-two fighting punch." — Nick Arcuri

And both Ameritech and BellSouth use authentication in combination with RF fingerprinting.

"RF fingerprinting and authentication provide a very good one-two fighting punch," BANM's Arcuri said. "And we still support the PIN (personal identification number), which we deployed early on before we could get authentication in the marketplace, although the PIN is clearly not as secure as authentication. We need to deploy solutions that work for our customers, but of course, one size doesn't fit all."

Whalen agreed that a multitiered approach is critical to fighting fraud.

"A multisystem attack is the best protection from the carrier standpoint," he said. "That's not to say that a carrier should go out and spend millions and millions of dollars to solve a problem. What they need to do is pick and choose from among the different types of products that are in the marketplace that will give them the biggest bang for the buck."

CHOOSE YOUR WEAPONS

If you're interested in a multisystem attack on fraud, you're in luck; there are several companies that offer a variety of fraud control systems. Here is a sampling of what's available:

• *Cellular Technical Services* provides Blackbird, a pr
variety of a
PreTect. PreTe
cifically desig
lem of fraudule
counterfeit or

• *Coral System*
fraud managen
tection and pre
that combats th
fraud, includin
does this by s
carrier's entire
basis. When th
in a subscriber'
diately notifies

"We've had g
Buster," said Cc
can't disclose
some of the con
indication of ou
customer base.
customer grow
and with the em
in the United S

• Also offering
Corsair Comm
Print fraud con
gerprinting tec
fies a unique
each time a call
techniques to v
fore the call is
two RF fingerp
illegal phone is
PhonePrint has
cloning fraud by
an entire cellula

• *GTE Telecom*
fers two fraud
FraudForce and
tem. FraudForce
carriers can cust
ing needs. It inc
which gives hon
block or restrict
markets; FraudC
automated verifi
carriers can avoi
high fraud mark
Protection Cent
organization.